INCREASING THE LEVEL OF NETWORK AND INFORMATION SECURITY

PU "Paisii Hilendarski" - Plovdiv
Author: Detelina Milkoteva

Abstract: "Need" gives birth to "Idea". Guided by this maxim, namely that my experience in school as a teacher of Web Design (in the search for security for websites in the Web space), my experience as Head of the Department of Information and Communication Technologies and of Physics (security technology is related to physics), are the reason I made this development. And as RNIKT I had to perform the tasks:

• to conduct internal trainings on cyber hygiene and good practices for network and information security at school; constant monitoring of the parameters of communication networks and systems for the presence of anomalies during operation;

• take measures to protect information and network devices;

• to prepare rules and an action plan in case of incidents;

• enforced password management policies;

• to search web security for websites etc.;

This training achieves the coordinated development of societal capabilities by engaging all stakeholders to counter intentional or unintentional threats to electronic information and respond adequately. Our modern times are very much accompanied by electronic processing of information. The information age passed into the cyber age - a time of modern electronic technologies and computer networks. Networks that connect not only the information system in the form of computers, but also in the form of so-called "smart" objects with an installed operating system. The variety and development of Internet devices is growing exponentially, which is a prerequisite for a cyber threat to the security of the operation of these billions of already networked devices. Organizing and implementing effective security requires a lot of time and labor for activity analysis, millions of lines of programming code.

The scientific direction that deals with increasing the level of information and network security, the protection of digital information in systems, is called Cybersecurity. In this cyber security development, almost all information security needs are covered, both in local networks and the Internet, and in the information systems themselves. Ensuring complete cyber security and subsequently achieving a strategic goal of cyber resilience requires a lot of effort from both network administrators and information security professionals, as well as developers. The purpose of the development is: To examine and analyze globally known cyberattacks and provide technical recommendations and measures to increase the level of information protection. In order to achieve the goal, it is necessary to study the nature, role, place and tasks of cyber protection in communication and information systems, to analyze the trends of existing threats, to study directions for optimizing the protection of communication and information systems. The OBJECT of examination is the information system with accompanying application programs and operating systems in the information terminals. The subject of consideration is the identification of cyber security vulnerabilities and countermeasures. Important on the topic is the summarization, systematization and integration of the various technical methods for cyber analysis and solving cyber defense problems. We will consider only the most famous cyberattacks with the greatest damage to information security, from the many decryption attacks only known password databases are indicated, for information terminals only the most used operating systems are considered.

Keywords: *risks, threats, vulnerabilities, cyber attacks, cyber security, malware, script, crypto resistance, critical points*

ПОВИШАВАНЕ НИВОТО НА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ПУ „Паисий Хилендарски“ Пловдив
Автор: Детелина Милкотева, *редовен докторант-отчислен*

Ключови думи: *рискове, заплахи, уязвимости, кибератаки, киберсигурност, зловреден софтуер-малуер, скрипт, криптоустойчивост, критични точки*

Резюме: *Настоящата разработка е посветена на повишаване нивото на мрежова и информационна сигурност. В нея се разглеждат, изучават и анализират най-актуалните кибератаки и се дават препоръки за повишаване нивото на защита на информацията. Изясняват се понятията „рискове“, „заплахи“, „уязвимости“, „кибератаки“, които са взаимосвързани. Дава се примерна схема-траектория на кибератака, нива на защита на информацията**,** видове пробиви-*

експлойти в системите, видове експлоатиращи действия, примери за зловреден софтуер, уязвимости в уеб приложения, киберзащита, подходи и мерки за защита на информацията.

ВЪВЕДЕНИЕ. "**Нуждата**" поражда „**Идеята**". Водена от тази максима, а именно че опита ми в училище като учител по Уеб дизайн (в търсенето на сигурност за уеб сайтовете в Уеб пространството), опитът ми като Ръководител на направление информационни и комуникационни технологии и на Физик (технологията за защита е свързана с физиката), са причина да направя тази разработка. И като РНИКТ трябваше да изпълнявам задачите:

- да провеждам вътрешни обучения относно киберхигиената и добри практики за мрежова и информационна сигурност в училище; постоянно следене на параметрите на комуникационните мрежи и системи за наличие на аномалии по време на експлоатация;
- да се вземат и мерки за защита на информацията и мрежовите устройства;
- да се изготвят правила и план за действие при инциденти;
- наложени политики за управление на паролите;
- да търся сигурност в уеб за уебсайтовете и др.;

С това обучение се постига координирано развитие на способностите на обществото чрез ангажиране на всички заинтересовани лица с цел противопоставяне на преднамерени или непреднамерени заплахи за електронната информацията и адекватна реакция. Нашето съвремие е съпътствано изключително много с електронна обработка на информация. Информационната ера премина в **кибер ера** – време на съвременни електронни технологии и компютърни мрежи. Мрежи, които свързват не само информационната система под формата на компютри, а и под формата на т. нар. „умни" предмети с инсталирана операционна система. Разнообразието и развитието на интернет устройствата нараства лавинообразно, което е предпоставка за кибер заплаха за сигурността на оперирането на тези милиарди вече мрежови устройства. За организирането и внедряването на ефективна сигурност са необходими много време и труд за анализ на дейността, милиони редове програмиращ код.
Научното направление, което се занимава с повишаване нивото на информационна и мрежова сигурност, защитата на цифровата информация в системите, се нарича **Киберсигурност**.

В тази разработка за киберсигурността, са обхванати почти всички необходими на информационната сигурност, както в локалните мрежи и Интернет, така и в самите информационни системи. За осигуряване на пълна киберсигурност и в последствие постигане на стратегическа цел за киберустойчивост са нужни много усилия, както от мрежови администратори и специалисти по информационна сигурност, така и от програмисти.
Целта на разработката е: **Да се разгледат и анализират световно известни до момента кибератаки и да се дадат технически препоръки и мерки за повишаване нивото на защита на информацията.**
За да се постигне целта е необходимо да се изследва същността, ролята, мястото и задачите на киберзащитата в комуникационно-информационните системи, да се анализират тенденциите на съществуващите заплахи, да се изследват направленията за оптимизиране на защита на комуникационно-информационните системи.

ОБЕКТ на обследване е информационната система със съпътстващите я приложни програми и операционни системи в информационните терминали.
Предмет на разглеждане е посочване на уязвимите точки на киберсигурността и мерки за противодействие. Важно по темата е обобщаването, систематизирането и интеграцията на различните технически методи за киберанализ и решаване проблемите по киберзащита. Ще разгледаме само най-известните кибератаки с най-големи поражения върху информационната сигурност, от множеството атаки по декриптиране са посочени само известни бази данни на пароли, за информационните терминали са разгледани само най-употребяваните операционни системи.

ПРИНЦИПИ И МЕТОДИ ЗА СИГУРНОСТ. МАТЕРИАЛИ - средства

Принцип - това е идея, мисъл, основна позиция. Метод - това е начин, начин за постигане на целта, основан на познаването на най-общите закономерности. Принципите и методите за осигуряване на сигурност се отнасят до частни, специални методи, за разлика от общите методи. Принципите на сигурност могат да бъдат разделени на ръководни, технически, организационни и управленски. **Ръководните включват:** принцип на операторска дейност, хуманизиране на дейността, унищожаване, подмяна на оператора, класификация, отстраняване на опасността, последователност, намаляване на риска. **Техническите включват:** принцип на блокиране, евакуация, запечатване, дистанционна защита, компресия, здравина, слабо звено, флегматизация, екраниране. **Организационните включват:** принцип на защита от време, информация, несъвместимост, нормиране, подбор на персонал, последователност, ергономичност.

Управлението включва: принципа на адекватност на контрол, обратна връзка, отговорност, планиране, стимулиране, управление, ефективност.

Принципът на нормирането е да се установят такива параметри, чието спазване гарантира защитата на човек от съответната опасност. Например МДК (максимално допустими концентрации), МДЕ (максимално допустими емисии), МДН (максимално допустими нива) и т.н.

Принципът на слабата връзка е, че за да се гарантира безопасността, в разглежданата система (обект) се въвежда елемент, който е проектиран по такъв начин, че възприема или реагира на промяна в съответния параметър, предотвратявайки опасно явление. Пример за прилагането на този принцип са спуканите дискове, предпазители и други елементи.

Принципът на информацията е предаването и усвояването на информация от персонала, чието изпълнение осигурява подходящо ниво на сигурност. Примери за изпълнение: ***обучение, инструкции, предупредителни етикети и др***.

Принципът на класификация (категоризация), се състои в разделяне на обекти на класове и категории според признаците, свързани с опасностите. Например: санитарно-защитни зони, категории на производство за опасност от експлозия и пожар и др. За да разгледаме методите за сигурност, въвеждаме следните дефиниции.

- **Хомосфера** - пространството (работната зона), където човек се намира в процес на разглежданата дейност.
- **Ноксосфера** - пространство, в което постоянно съществуват или периодично възникват опасности.

Комбинацията от хомосфера и ноксосфера е неприемлива от гледна точка на сигурността.

Сигурността се осигурява чрез три основни метода: А, Б, В.
Метод **А,** се състои в пространственото и (или) временното разделяне на хомосферата и ноксосферата. Това се постига чрез дистанционно управление, автоматизация, роботизация и др.
Метод **Б,** се състои в нормализиране на ноксосферата чрез елиминиране на опасностите. Това е набор от мерки, които предпазват човек от шум, газ, прах и други средства за колективна защита.
Метод **В,** съдържа набор от техники и средства, насочени към адаптиране на човек към подходящата среда и повишаване на неговата сигурност. Този метод реализира възможностите за професионален подбор, обучение, психологическо въздействие, лични предпазни средства.

В реални условия, като правило, тези методи се използват заедно или в различни комбинации.

Напоследък основна тенденция в развитието на системите за контрол на достъпа е тяхната интелектуализация и интеграция с други системи за сигурност. Системата ACS включва голям брой подсистеми, които могат да работят напълно автономно (и т.н.) и могат да взаимодействат с всички системи за контрол на достъпа и други системи за сигурност (например система за контролни точки - оборудването ACS взаимодейства: ***турникет, четци, контролери , софтуерен пакет и система за видеонаблюдение: видеокамера и софтуер, който осигурява допълнителен запис, идентифициране на лице и записване на факта на преминаване през контролно-пропускателния пункт към архива)***. ACS системите осигуряват събиране, обработка и отчитане, използвайки значително количество информация и я прехвърлят към главния компютър (сървър), всъщност в интегрираните системи за сигурност те изпълняват една от централните функции, благодарение на информацията, получена и предадена от ACS, функциите и регулациите са конфигурирани за работата на други системи, като видеонаблюдение, охранителна и пожарна аларми, периметърна охрана, осветление, вентилация, отопление, комуникации и т.н. точно тези помещения, до които на служителя е разрешен достъп, осветлението в инсталираните помещения се включва автоматично, отоплението се включва, в зависимост от броя на служителите, които са дошли, режимът на вентилация се променя и т.н.)

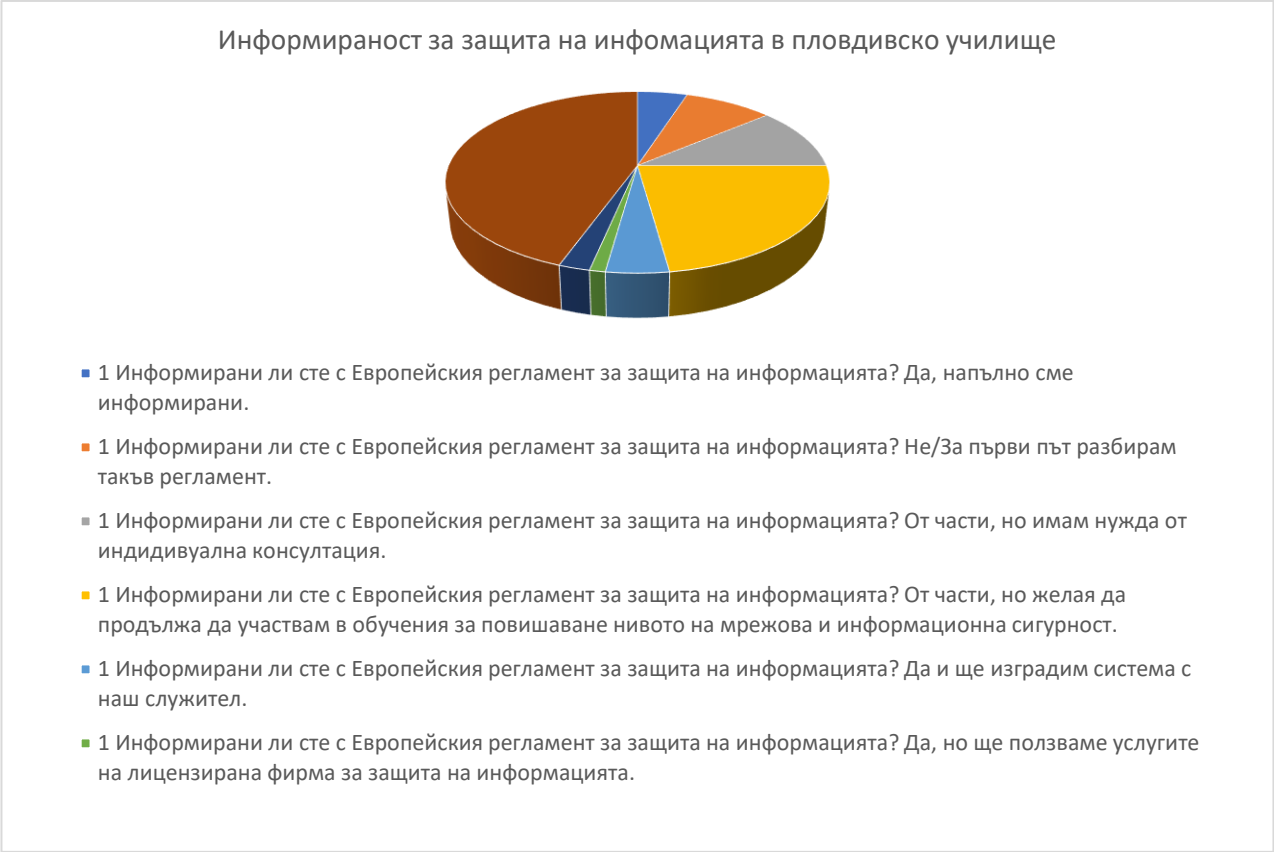
РЕЗУЛТАТИ

След направена анкета, се вижда, че много малко хора са запознати с Регламента за защита на информация. В тази връзка направих инструктаж на служителите в училище за повишаване нивото на сигурност и защита на информацията.

№	*Въпроси*	*Отговори*	*Отговори в %*
1	**Информирани ли сте с Европейския регламент за защита на информацията?**	*Да, напълно сме информирани.*	**9%**
		Не/За първи път разбирам такъв регламент.	**16%**
		От части, но имам нужда от индидивуална консултация.	**20%**
		От части, но желая да продължа да участвам в обучения за повишаване нивото на мрежова и информационна сигурност.	**41%**

		Да и ще изградим система с наш служител.	**8%**
		Да, но ще ползваме услугите на лицензирана фирма за защита на информацията.	**2%**
		Друго (Моля, посочете).	**4%**
2	**Информирани ли сте от РНИКТ за защита на информацията във Вашето звено?**	*Да, напълно сме информирани.*	**80%**
3	***От колко човека е колектива?***	94	**94**

Таблица 1. Проведена анкета за информираност за защита на информацията



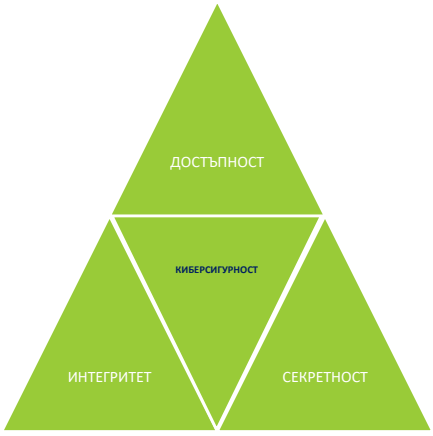
Фиг. 1 Информираност за защита на информацията

Хипотеза. Очаква се да се повиши нивото на информационна и мрежова сигурност.

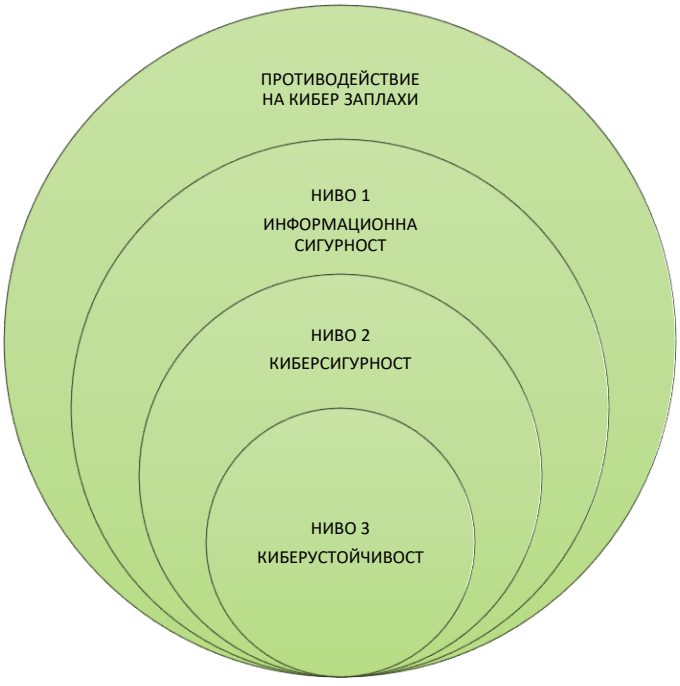
I. КИБЕРЗАПЛАХИТЕ В ИНФОРМАЦИОННИТЕ – КОМУНИКАЦИОННИ СИСТЕМИ

1. **Съвременна тенденция в комуникационно-информационните системи е киберсигурността,** което представлява състояние на обществото и държавата, при което чрез изграждане на правила, и поддръжка на активни и превантивни мерки и действия, които защитават информационна и мрежова сигурност.

България към момента следва политиката на Европейския съюз и в своите регламентирани документи и по-точно в Европейската рамка за Киберсигурност, под понятието киберсигурност се посочват: предпазни мерки и действия, които могат да бъдат приложени за предпазване на киберпространството, както в гражданската, така и във военната област от заплахи, които са свързани с независими мрежи и информационна инфраструктура или могат да нарушат работата на тези мрежи. Целта на тези мерки за осигуряване на киберсигурност е запазването и поддържането на наличността, поверителността и целостта на електронната информация, която непрекъснато се обменя под различна форма в мрежата и комуникационната инфраструктура. Овладяването и възстановяването от кибератака е ново ниво на зрялост, известно като киберустойчивост. Високата киберустойчивост подготвя хората за „Неизвестните неизвестни“ и включва защита и ограничаване на пораженията, максимално запазване и функциониране, възстановяване на услуги и дейности. Достигането на това ниво е всъщност е всъщност **следващото ниво, а именно сигурност и надеждност на всички компоненти и активи в киберпространството – информация, техника, хора и съоръжения, комуникационни канали, системи и услуги, надеждната им свързаност и оперативна съвместимост.**



Фиг. 2 Информационна сигурност и концепция за киберустойчивост.



Фиг. 3 Нива на защита на информацията и технологията в мрежова среда.

Тенденцията посочена в националната стратегия, е достигането на зряла общественост и *киберустойчивост*. За постигане на целите е необходимо точно и ясно да се дефинират реално съществуващите заплахи, както и същността, ролята, мястото и задачите, пред защитниците на информацията. Свръх широкото използване на компютърни мрежи и операционни системи от ново поколение, предлагащи непрекъсната свързаност с устройствата и „неизвестните неизвестни“ от Интернет, както и развитието на инфраструктури, обработващи огромни база от входни данни (Big Data), крие рискове за среща с киберпрестъпниците и киберопасностите.

Слабите точки при програмиране на приложения, опериране на системи и настройване на мрежови устройства са уязвимостите и основното направление за пробив в компютърната и мрежовата сигурност. Често голям процент от потребителите отварят писма по електронната си поща, съдържащи злонамерен код. Този процес се нарича, фишинг (e-mail. phishing). Ярък пример е атаката към информационните масиви на НАП – агенция по приходите. И докато в България опасността от телефонни измами продължава да съществува, то в световен мащаб заплахата е от лъжливи електронни писма, които карат потребителите да кликват върху изпълними прикачени файлове или върху препратка към зловреден уебсайт. Изводът е, че човешкият фактор остава най-уязвим за комуникационно-информационните системи от гледна точка на киберсигурността. Благодарение на изтънчените технологии – операции в комуникационните мрежи и системи, позволяват от дистанция да се премахват киберзаплахите, които застрашават гражданите, функционирането на държавата, икономиката, обществото, науката и образованието. Тези кибератаки се осъществяват най-вече от отдалечен компютър – информационна система. Целта им е с откриването на прости и ефективни уязвимости в софтуерната и в хардуерната конфигурация да причинят значителни поражения с нанасяне на финансови, материални, а понякога дори и човешки загуби. Кибератаките нямат национални, културни или юридически граници. Рисковете и заплахите в киберпространството са трудни за дефиниране, поради сложността за определяне на източника на въздействие, целите, мотивите, бързото скалиране на заплахата и трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси. Най-въздействащите са **хибридните атаки – комбинация от кибер и физическа атака**. Така е например кибератака, целяща критичен кинетичен процес, или кибератака при бедствие, по време на неизправност в критична информационна система. Обект на такива атаки са публичния, частния сектор и гражданите. Реакцията от последващи атаки налага координирани действия и превантивни мерки за минимизиране на възможностите за прерастване в кризи, както и за адекватни последващи действия, които да доведат до възстановяване на нормалното функциониране на системите. Нужно е да се инсталира специализиран софтуер, но може да има проблем със съвместимостта на останалите приложения и операционни системи. Човешкият фактор влиза в действие, запознатите в дълбочина с анатомията на операционните системи, без значение коя е тя, чрез задълбочени анализи могат да разберат достатъчно за наличието на нерегламентираните активности и да приложат мерки за противодействие с инциденти по сигурността. Източници на организирани кибератаки може да са държави, военни и терористични организации, индустриален шпионаж, кибер престъпници, хакери, кракери и др. Мотивацията може да е от икономически ползи, любопитство, хулиганство, демонстриране на надмощие и др. Значителна част от кибератаките са престъпления с цел най-вече **Финансови облаги** от различно естество. Може да има кибератаки с цел тормоз, измама, разпространяване на детска порнография, нарушаване правата на интелектуалната собственост и много други. По природа кибератаките са „**асиметрични**“ – с малки усилия и средства нанасят големи поражения и с непредсказуеми. Именно за това киберпространството е привлекателна среда, поради отдалечения достъп и липсата на ефективно правораздаване по отношение на киберпрестъпността. Огромното разнообразие от кибератаки прави противодействието по-сложно. Напоследък действията на киберпрестъпниците са далеч по-изтънчени, имат значителни ресурси и капацитет и усъвършенстване на разпределението на роли и взаимодействие между криминалните мрежи.

2. **Заплахите за сигурността – основни определения:** Понятията „рискове“, „заплахи“, „уязвимости“, „кибератаки“ са взаимосвързани.
    - „Заплахата„ представлява възможността за протичане на опасно събитие – атаки. Това събитие е унищожително.
    - „Уязвимостта“ е слабост, която прави целевата компютърна система или мрежа податлива на кибератаки. Тя е слабост, определяща дадена цел да бъде податлива на атака.
    - „Кибератака“ – действие по изрично пробиване в уязвимото място.
    - „Атака“ е целенасочено експлоатация върху открита слабост в компютърните системи.
    - „Зловреден софтуер“ или „малуер“, се използва за описването на компютърни програми, нарушаващи дейността на компютъра или чрез, които се добива достъп до компютърните системи без знанието или разрешението на потребителя. Те са изключително трудно засичани и разпознавани като такива. Други такива видове злонамерен код са вируси, червеи, заек, троянски коне. Но за да има успех една кибератака, са нужни факторите:

- агенти на атака;
- посока;
- уязвимости в управлението;
- уязвимости в защитата;

- техническо влияние. Ето и схема:

Фиг. 4 Траектория на провежданата кибератака като риск за киберсигурността на мрежовата и информационна сигурност

Обекти на атаки, може да се окажат съвременни комуникационни системи, например SCADA (Supervisory Control and Data Asquisition) – платформа за събиране и обработка на данни в реално време, както и запис на събития под формата на журнали от ОС. Могат да комуникират директно и да взаимодействат с различни устройства като сензори, клапани, помпи, мотори, осветление, което става посредством управление чрез интерфейс човек-машина, а това може да се окаже уязвимост за неправомерен достъп.

3. **Видове пробиви-експлойти в системите:** Експлойтът отваря комуникационните пробойни, наречени „входни вратички“ към КС, като може да причини злонамерено дистанционно управление на целевата машина, кражба на информация, допълнително записване, инсталиране или активиране на зловреден софтуер. Те са два вида експлойти:
    - **Remote(отдалечен)**
    - **Local (местен, локален)**
4. **Видове експлоатиращи действия**
    - **Malware** – тайно управление на КС, без знание на потребителя;
    - **Denial-of-Service** - отказ на услуги.
    - **Cross-Site** - инжектиране на код;
    - **SQL Injection** - манипулира БД;
    - **Phishing** - атака към потребители или цели;
    - **Credential reuse** – използване на събрани пароли, потребителски имена;
    - **Spear phishing attacks** – насочени към фирмени лога, ел. писма;
    - **Whaling phishing attacks** – към шефове на организации;
    - **Brute – Force** – крадене на акаунти;
5. **Зловредния софтуер в ИКС – става въпрос за телефонните измамници.** Целта им е, чрез специални тонове в телефонна слушалка да се придобие безплатен достъп до мрежов ресурс.
    - **CIH** – дълго време стои в КС без активност.
    - **Melissa** - разпространява се чрез съобщения по имейл.
    - **Червей “I love you”** – скрипт, който като се стартира разнася множество копия, задръстват трафика, трият се важни файлове.
    - **Червей “Code Red”** - атакува уебсайтовете;
    - **Virus “Conficker”**- отгатва пароли от ОС Уиндоус;
    - **Virus “Stuxnet”** – заразява компютри за управление на контролери, дейност на механизми;
    - **Virus “Flame”** – кибершпионаж;
    - **Virus „Петя“** – криптира, не позволява на ОС да се зареди;
    - **SolarStorm** - заразява доставчика на услуги;

Хакерите продължават да се опитват да пробиват системи и приложения по различни начини. Що се отнася до инструментите за изследване на киберсигурността, излиза понятието „Етично хакерство“. ОС Кали Линукс е най-известната ОС и най-желана от специалистите по киберсигурност.

ИЗВОДИ: КИБЕРАТАКИТЕ придобиват все по-големи мащаби поради множество бизнес процеси – онлайн пазаруване, комуникации, банкиране, хостинг, облачните технологии, предаване на съдържание и др. Има атаки от вида на блокиране

на мрежата и реализиране на огромен брой заявки и др. Съвременните КМ са изградени на базата на цифрова обработка на сигналите, множество видове отделни комуникационни протоколи и сложна йерархия, разделяща функционалността в обработката на потребителските данни.

За идентифициране, локализиране и оценка на уязвимостите, са разработени специализирани софтуерни инструменти, методологии и технически инструкции. Уязвимостите са IP камери, рутери, дисплеи за управление на климатици и др.

Уязвимости на ОС Win10: уязвимост в драйверите, при отдалечено изпълнение на код, когато ОС неправилно обработва данните, в стека за протокол http съществува уязвимост от отказ на услуга, уязвимост от повреда на паметта, уязвимост от вида на сайт-скриптовете, хостинг услугите и др.

6. **Уязвимости в уеб-приложения:** една от основните уязвимости в използвани приложения в съвременни КМС е нерегламентирано вмъкване на код в отворени форми, които се използват за попълване на формуляри и придават **интерактивност на уеб сайта**. **Всеизвестно е, че езикът за програмиране JavaScript придава живина и интерактивност на уебсайта.** Но функционирането на скриптовете са уязвими точки не само към сървъра, а и към клиентската част в инструментариума на интернет браузъра. При кражба на данни от сървърната част, хакерите и кракерите могат да заразяват клиентската част с малуер посредством открити уязвимости в приложния код.

ВАЖНО!!! Една от най-популярните инструменти за изследване на уязвимости е **OWASP** ZED Attack Proxy – ZAP. Той се поддържа активно от стотици международни доброволци и това помага автоматизирането при търсене на уязвимости в уебсайтове и уеб приложния. КИС са изложени на риск при неподдържана или неправилна експлоатация. Лесно може да се сдобият с информация всякакви кракери. Съществуват множество пътеки за повишаване нивото на заплахи към информационната сигурност. Спасението е непрекъснат процес на обучение, следене и адекватен отговор на възникналите заплахи.

II. КИБЕРЗАЩИТА

Мрежовият достъп е уязвимия момент. В кабелните мрежи, „пробиване“ трудно се постига, но при безжичните е много лесно. За това е нужна политика за киберсигурност в работна среда с КМ и тя трябва да съдържа аспектите:

- Концепция за пълна защита на информацията в мрежата;
- Стратегически цели за осигуряване на безопасност и защита на електронната информация;
- Обученията;
- Висока Величина на отговорност и задължения на работещите в организацията;

Нужно е да се изгражда киберархитектура, която моментално да отразява моментното състояние на потребностите и целите на системата и киберзащитата трябва да покрива целия спектър от уязвими места и **критични точки**.

III. ОСНОВНИ ПОДХОДИ ПРИ ЗАЩИТА НА ИКС

1. **Подходи при защита:** В съвременния етап от развитие на техниката технологиите чрез използване на системи от сигнали със сложна честотно-времева структура е възможно едновременно да се осигури сигурност на информацията и скритост, от една страна и висока шумоустойчивост от друга. След откриването на електромагнитното излъчване на радиокомуникационните системи-РКС и определяне на параметрите на сигналите може да започне радиоелектронната скритост-РЕС. Използват се за скриване на информацията със средствата:

- **Активните смущения** се създават обикновено от радио и инфрачервения диапазон. По своя честотен спектър, те се делят на **прицелни**, **заградителни** и **пълзящи**, а принципа на въздействие върху подаваните радиоелектронни средства – на ***максиращи*** (шумови) и ***имитационни***. Заградителните смущения се излъчват в широк честотен диапазон, изискват приблизително познаване на работната честота на подаваното средство, обаче е необходима значително по-голяма излъчвана мощност. Пълзящите съчетават предимства на прицелните и заградителните. То се създава от шумови генератори с тясна лента на излъчване, които плавно се пренастройват в рамките на подавания честотен диапазон. Шумовите смущения изкривяват параметрите на полезните сигнали и в резултат се скрива процесът на обработка на приетите сигнали. Имитационните смущения са преднамерено излъчване на радиосигнали, които създават лъжливи обекти, претоварването с изображенията върху мониторите и пунктовете за наблюдение и контрол.
- **Пасивни средства** за РЕП – базират се на явлението „разсейване на електромагнитите вълни“ от различни отразяващи повърхности, които пренасищат изображенията върху монитора. Лъжливите изображения и обекти имитират истински обекти. Те се създават чрез радиоотражатели, пасивни агентни решетки и дистанционно управляеми самолети – дрон или колички.

- **Мощните йонизиращи лъчения** могат съществено да нарушат работата на РКС чрез изменение на условията на разпространение на електромагнитни вълни в йоносфрета. Сриват функционирането на електроните и полупроводниковите прибори.
- **Стелт технологиите** имат за цел намаляване ефективността на радиолокационните системи чрез намаляване на „видимостта“ на обектите чрез специално оформяне на корпусите им, покриване с радиопоглъщащи материали и др.
- **Непреднамерените смущения** са смущения с променлив и естествен произход. Те обективно улесняват действията на противника, тъй като пречат на работата на РКС и другите КС.

ИЗВОД: Използването на РЕП от лица, престъпни групи влияе отрицателно на РКС. Следва РЕЗ – радиоелектронна защита да бъде комплексна и всеобхватна, а РКС да са построени на технически принципи, така че злонамерените лица да бъдат максимално затруднени в организирането и провеждането на радиоелектронното противодействие – РЕП.

2. **Роля на криптографски методи за защита на информация:** информационната скритост се нарича **криптоустойчивост**, което важен научен проблем. Криптографията създава концепциите, методите и средствата за конфиденциалност, цялостност, идентификация и автентификация. Криптографска система е технология за скриване смисъла на информацията от неправомерен достъп. Наука, която създава такива технологии, се нарича **Криптография**. А **Криптоанализът** е изкуство за разкриване, разбиване на криптосистеми. Терминът „криптология“ произлиза от гр. дума „криптос“ – скрит.

Криптоустойчивостта се изразява в способност да противостои на атаки на криптоаналитиците!

Информационната скритост е способност на РКС да противостои на мерките, насочени към разкриване смисъла на подаваната информация.

IV. МЕРКИ ЗА ЗАЩИТА СРЕЩУ КИБЕРАТАКИ

1. Защита от нерегламентиран достъп и кражби на конфиденциална и класифицирана информация;
2. Предотвратяване на опитите за промяна на съществуващи данни, заличаване, триене;
3. Формиране на киберхигиена за безопасна работна среда с ИКС;
4. Защита при използване при електронна поща и социални мрежи;

Техническите средства са хардуерна и софтуерна защита на ИКС:

1. Средства за физическо осигуряване на КС срещу кражба, несанкциониран достъп и некоректно използване;
2. Средства за контрол на достъпа – защитни стени, пароли, задаване на биометрични данни;
3. Средства за превенция-откриване на непозволени пробиви NIDS;
4. PKI – частни ключове, средства за кодиране;
5. Средства за автентификация – цифрови сертификати, маркери, електронни подписи;
6. Средства за защита от въздействие от електромагнитни смущения и импулси – екраниране EMI/RFI;
7. Средства за контрол на мрежата – подходящи софтуерни и хардуерни средства като скенери, снифери - сменя MAC адреса на компютъра ,и по този начин спира интернета на цялата мрежа;
8. За защита на **уеб сървъри трябва да се инсталират сертификати от доверени системи – TLS, TTPS.**
9. Защита на крайните мрежови устройства – трябва да се обръща внимание на абсолютно всички обстоятелства и процеси, свързани с използването на съответното крайно устройство;
10. Защита на устройства с ОС Win: като Уиндоус е най-известната и най-разпространената система, тя е обект номер 1 на кибератаки. Microsoft се грижи, но има и препоръки: ъпгрейд на програмите към тяхната последна версия, криптиране на данните в Win 10, Update Assistant.
11. Win10 – криптиране на данни: включване на BitLocker; Search/BitLocker (control panel/System and Security/BitLocker Drive Encryption);
12. Memory Integrity – включване на функцията за цялостност на данните. Ако се прави запис на данни върху дяловете на ОС, се изчислява под формата на хеш-стойност, която определя каква информация е записана и в какво състояние е ОС след използването й. Ако при последно сравнение на хеш-стойностите не съвпадат, то е имало промяна на паметта. Отново от win Security.
13. Включване на защита от вируси - AVX;
14. DMZ, IPS/IDS – защитни стени;
15. Мулти-агентни интелигентни системи Smart Grid Distributed Intrusion Detection System (йерархична система, откриваща и класифицираща зловредни кодове и кибератаки);

ВНИМАНИЕ! Най-слабото звено в една инфраструктура си остава личността, за това е силно препоръчително да се осъществяват обучения, да се спазват задълженията. Киберсигурността е високоскоростен процес и е необходим ресурс от образовани хора, техника, софтуер, време. Пътищата за атаки са много и разнообразни, а най-ценния актив е времевото постоянство и своевременната отговорност на киберзаплахите. Ето и следните ПРАВИЛА:

- Ползвайте повече от една парола;
- Пазете картовите си данни;
- Обръщайте внимание на заглавието на имейла; Ако съдържа граматически грешки или има несъответствия на вашия роден език – пратете го в кошчето, без да го отваряте;
- Следете отблизо профила си в банката; В случай на подозрителни трансакции, свържете се с вашата банка. Проверявайте трансакциите по банковата си сметка поне веднъж седмично. Най-лесно това става с мобилно и онлайн банкиране. С банката в телефона ви за секунди можете да следите наличността по сметката си отвсякъде и по всяко време;
- Внимавайте с линкове и прикачени файлове;
- Проверявайте кой ви изпраща съобщението;
- Бъдете внимателни, когато използвате обществени wi-fi мрежи;
- Правописните грешки често са предупредителен знак;
- Фишинг имейлите често съдържат правописни грешки в текста или малки грешки в изписването на предполагаемото име на подателя;
- Винаги актуализирайте софтуера на устройствата си;
- Използвайте силни пароли;
- За случаите, когато сте извън офиса
- Включете в пощата си автоматичното изпращане на съобщения само за получатели в рамките на своята работа, но не и за външни получатели. По този начин ще избегнете потенциални хакери да узнаят, че няма да ви има за известно време.
- Винаги проверявайте URL адреса. Ако сайтът включва "https: //, тогава на сайта може да се има доверие и е защитен. Ако URL адресът е " http: // и липсва последната буквичка "s", то тогава избягвайте да въвеждате чувствителна информация като номера на вашата кредитна или дебитна карта, пароли и т.н.
- Внимавайте в социалните мрежи.
- Спазвайте етичен интернет етикет.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. https://itstep.bg/category/blog-bg/kakvo-e-kibersigurnost-i-kak-da-se-predpazim-v-internet-prostranstvoto
2. Международна сигурност; Автор: Веселин Целков, Николай Стоянов, Орхан Исмаилов;
3. Киберсигурност – университетско издание гр. Шумен, Автор: доц. д-р инж. Росен Атанасов Богданов и др.;
4. Въведение в криптографията и сигурност на данните, поредица „Защита на информацията“, Автор: Веселин Целков, Николай Стоянов, Орхан Исмаилов;
5. Уикипедия – оторизиран и често проверяван уеб сайт

РЕЧНИК

КИС – компютърни информационни системи, ОС – операционна система

КС – компютърна система, ИКС – информационни и комуникационни системи

БД – база данни, КМ – комуникационни, компютърни мрежи

КМС – компютърни мрежи и системи

РЕС – радиоелектронна скритост, РКС – радиокомуникационна система

РЕП – радиоелектронно противодействие, РЕЗ – радиоелектронна защита

Превенция-откриване, РНИКТ – Ръководител на направление Информационни и комуникационни технологии

Интегритет - от лат. “непокътнатост, цялост; непоквареност, честност”

ст. учител в ОУ „Яне Сандански“ Пловдив
detelina_milkoteva@abv.bg